EXHIBIT 60

MAO DECLARATION
ISO PLAINTIFFS'
MOTION FOR CLASS CERTIFICATION

DOCUMENT SOUGHT TO BE SEALED

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ANIBAL RODRIGUEZ, SAL CATALDO, JULIAN SANTIAGO, and SUSAN LYNN HARVEY, individually and on behalf of all other similarly situated, Plaintiffs, v. GOOGLE LLC, Defendant.	No. 3:20-cv-04688-RS

REBUTTAL EXPERT REPORT OF JOHN R. BLACK, PH.D.

May 31, 2023

h. "Google can pull the wool over its users' eyes, leaving them unaware that Google collects and saves their app activity data even when they have turned off WAA and sWAA."[68]

i. "Google in this case has relied on the relationship between app developers and users to try to excuse the fact that Google offers no way for users to delete WAA-off and sWAA-off data."[69]

B. Mr. Hochman's descriptions and opinions concerning Google's collection and saving of sWAA-off data are inaccurate.

1. Collection on Android and iOS

61. Mr. Hochman opines in his opinion A of Section VII of his report that Google "has collected WAA-off and sWAA-off data throughout the class period."[70] This opinion is peppered with further assertions regarding how Google uses the data, but his main opinions about usage of sWAA-off data come later in his report. I will address that aspect of his opinions later in this report.

62. The main point of Mr. Hochman's Opinion A is that Google Analytics for Firebase functions as designed vis-a-vis the app developer's data even when a Google account holder who has sWAA-off uses that app developer's app. In other words, the sWAA control does not change whether or not Google provides its analytics service to third party app developers. On this, Mr. Hochman and I agree. The Google Analytics for Firebase SDK is designed to help app developers understand how their users engage with their app with aggregated metrics such as

[68] Hochman Report, ¶ 144.
[69] Hochman Report, ¶ 255
[70] Hochman Report, ¶ 81.

time spent on particular articles or the geographic distribution of an app's users. This is all publicly documented functionality.[71]

63. Subject to other technical caveats not relevant here, when a GA4F user is also a Google account holder and Google has a way of checking to see that the account holder has sWAA turned off, the GA4F data the user generates is sent to Google and logged by Google in pseudonymous form on the app developer's behalf subject to the terms of use between Google and the app developer.[72] As described elsewhere herein, because the account holder had sWAA off and Google has a way of knowing that, it will not use the data to augment any marketing profile on that user, and therefore not use the data for targeting the user with particular advertising or personalizing the user's experience on Google products or services, in accordance with the WAA and sWAA control descriptions, which explain that the feature is meant to permit Google to save activity data to a user's account to use it for personalization.[73]

64. Mr. Hochman defines "WAA-off data" for purposes of his report as meaning "data generated during a user's interaction with a non-Google mobile app while that user is signed into a Google account and her WAA toggle was set to 'off'".[74] He defines sWAA-off data

[71] *See* Google, Google Analytics, Firebase, https://firebase.google.com/docs/analytics ("Google Analytics helps you understand how people use your web, Apple, or Android app. The SDK automatically captures a number of events and user properties and also allows you to define your own custom events to measure the things that uniquely matter to your business.").Google Analytics helps you understand how people use your web, Apple, or Android app. The SDK automatically captures a number of events and user properties and also allows you to define your own custom events to measure the things that uniquely matter to your business.").

[72] *E.g.*, Google's Supplemental Responses & Objections to Plaintiffs' Interrogatories, Set 7 ("Interrogatory Response, Set 7"), Interrogatory No. 23, at p. 18 ("When a user is logged into their Google Account and has turned WAA and/or sWAA off, any data that is collected by the Google Mobile Ads SDK is logged against pseudonymous identifiers."); *see also* Langner Tr. 185:13-17 ("For Google Analytics for Firebase data, when the user has sWAA-off, the Google Ads systems can use data in this pseudonymous space for the purposes of conversion measurement[.]").

[73] ROG 1, p. 23-26; Ganem Depo 68:21 -74:5; Hochman Report, ¶¶166, 250.

[74] Hochman Report, ¶ 82.

with Google accounts who were not under thirteen years of age and whose accounts were set up by that user as a standard consumer account, which Mr. Hochman also refers to as "consumer accounts."[76]

a. Google Analytics for Firebase

67. Mr. Hochman opines that "WAA and sWAA settings have no impact on the types of data collected by Google app analytics products."[77] As to GA4F and the analytics products incorporated into the GMA SDK, Mr. Hochman is partially correct. Throughout his report, Mr. Hochman mixes the concepts of collection, saving, and using. For example, in the next sentence, he discusses collection and saving in the same sentence. This conflation makes it difficult as a technical matter to opine accurately about Google's technology. In this report, I will carefully separate those concepts.

68. The types of app activity data sent to Google by apps that use GA4F and the GMA SDK are the same regardless of the user's account-level sWAA setting: they are the app activity data the app developer has requested Google collect for their analysis of their own apps and the way users use them. The infrastructure supporting the collection of data in GA4F and GMA SDK are the same.[78] As a result, in this report, whenever I refer to GA4F analytics functionality, that applies equally to the analytics functionality incorporated into the GMA SDK.

69. How the data sets are saved and used by Google differ depending on the user's sWAA setting. The app activity data sent to Google by GA4F is described in Google's interrogatory responses and in Mr. Hochman's report. It is also publicly documented by Google in its Firebase help center pages. At a high level, as Mr. Hochman describes, GA4F logs events

[76] *See e.g.*, Hochman Report, ¶ 39

[77] Hochman Report, ¶ 87.

[78] Google LLC's Fourth Supplemental Responses and Objections to Plaintiffs' Interrogatories Set One, Interrogatory No. 3, at 46.

to the user's device (either to a central log on Android or to an app-specific log on iOS), and those logged events are later uploaded to Google servers for consent checks, processing, and saving. On this, Mr. Hochman and I agree.

70. Standard GA4F events are, as Mr. Hochman describes, items like "first open." Google lists the current automatically collected events by GA4F on its Google Firebase support documentation.[79] These events are logged by GA4F with accompanying information; Mr. Hochman's report contains samples of the information first collected by GA4F at Hochman Appendix H.1 and H.2, and complete data productions of those initial collection logs as they pertain to Mr. Hochman's test devices were produced at GOOG-RDGZ-20833 and -834.

71. The way GA4F events are logged implies that an event occurred, but does not necessarily imply anything in particular about that event. For example, the "first_open" event is triggered "the first time a user launches an app after installing or re-installing it," and stored with that event is the device information (*e.g.*, ADID or IDFA, resolution, device type, etc.) and a timestamp.[80] The way GA4F logs this event does not contain any information about what the user saw or did on the app; only that the user opened the app at the given time. Another example: the event "screen_view" indicates that the app loaded a particular screen of the app at a given time.[81]

72. It is important to realize that how these events are customized is up to the app developer, and app developers can also create custom events of their own. Mr. Hochman does not acknowledge in his report that event parameters designed by an app developer may mean

[79] "[GA4] Automatically collected events", Analytics help, available at https://support.google.com/analytics/answer/9234069?hl=en.

[80] "[GA4] Automatically collected events", Analytics help, available at https://support.google.com/analytics/answer/9234069?hl=en.

[81] "[GA4] Automatically collected events", Analytics help, available at https://support.google.com/analytics/answer/9234069?hl=en.

evidence and Mr. Hochman's own report that AdView is terminology Google uses to name a log that contains ad impression data.[107]

91. An ad click is what it sounds like: a record that a user clicked (or tapped) on an ad shown in a third party app or other advertising surface, such as a website. Here again, the ad click entries in the record include information about the device displaying the ad, the app displaying the ad, and the format of the ad.

92. From my review of the adEvents log entries Google produced, I do not see any information in the entries that could be considered "app activity" information, as none of it relates to the activity the user engages in within the third party app serving the ad. The recording of ad requests, impressions, and clicks alongside device information, timestamps, and other similar record information is all directed at making a record that a user was shown or interacted with an ad, so that the advertiser whose ad it is can know that. In this way, Google serves as a bookkeeper for the advertiser. I am not aware of any use Google makes of sWAA-off adEvent data other than to calculate conversions, as Mr. Hochman describes. And that calculation simply connects the advertiser's interaction with the user at time 1 with another interaction with the same advertiser at time 2.

93. Next, Mr. Hochman opines that ad events data include identifiers. From my review of the entries Google produced and the related evidence, I agree that ad events data can include identifiers, and typically will include either a pseudonymous identifier such as ADID or IDFA (when sWAA is off) or a GAIA (when sWAA is confirmed on). These identifiers can

[107] Hochman Report, ¶ 122 (Google Mobile Ads SDK sends data to "several types of ad events," including "ad views, in which the user views an ad displayed in the app[.]").

facilitate the task of reporting to an advertiser that the same ADID that clicked on an ad at time 1 ultimately installed the advertiser's app at time 2.[108]

94. Mr. Hochman opines in connection with his opinion on the collection of data via the GMA SDK that "If Google did not collect and save ad requests, it could not serve ads."[109] It is unclear what he means here, but if he means that, to honor the sWAA control, Google would have to refuse to serve ads to confirmed sWAA-off devices through AdMob or Ad Manager, I see no evidence in the record that this is how anyone else understood the sWAA toggle. Not only is the ad events record information not app activity data, but in my opinion it would be unreasonable to assume that the sWAA toggle as described should function, in effect, as an ad blocker across apps and the Internet wherever Google serves ads.

c. Firebase Cloud Messenger

95. Mr. Hochman opines briefly that "Google collects a variety of information via Firebase Cloud Messaging, including several types of events, parameters, and user properties."[110] Here, again, Mr. Hochman does not explain how these data types are used, why they are collected, or what privacy violation Plaintiffs allege could be derived from the use of FCM by its design.

96. Indeed, I am unaware of any evidence that Google uses the FCM data Mr. Hochman describes in his Appendix I ¶ 58-62 (as evidence of sWAA-off collection of FCM

[108] Mr. Hochman fails to note that there is a collection toggle on Android and iOS devices that would prevent the collection of the ADID or IDFA corresponding to the mobile device: on Android, this is known as OOOAP, or Opt Out of Ad Personalization. Google's Fourth Supplemental Responses and Objections to Plaintiffs' Interrogatories Set Seven, Rog 25, p. 20. On iOS, this is known as LAT, or Limit Ad Tracking. *Id. See also* "Limit Ad Tracking," Singular, https://www.singular.net/glossary/limit-ad-tracking/. Since iOS 14, this has instead been known as ATT, or App Tracking Transparency. Google's Fourth Supplemental Responses and Objections to Plaintiffs' Interrogatories Set Seven, Rog 25, p. 7. In all cases, users have a device-level setting that can prevent the collection of this identifier.

[109] Hochman Report, ¶ 122.

[110] Hochman Report, ¶ 132.

214. I understand and agree with Mr. Hochman that "Google maintains a database which reliably shows which Google account holders turned off WAA and sWAA during the class period, and when those users did so."[275] That narrows the potential class to individuals who turned sWAA off. But this is where the line of inquiry ends. Mr. Hochman asserts that "Google can also locate in its records users' devices associated with each Google account, which means that Google knows which of its account holders have used a mobile device during the class period."[276] That is not correct. For this proposition, Mr. Hochman relies on Section VII.B.1 of his report, but that section of his report is merely a description of Google's data infrastructures, and does not discuss whether Google can reliably identify the mobile devices used by every Google account holder with sWAA off at any point during the class period.

215. Mr. Hochman's next paragraph states instead that users can self-identify if they used a mobile device with sWAA off. In this, Mr. Hochman abandons his opinion that Google can identify class members.[277] Mr. Hochman surmises that users can identify a list of apps they've used, and Google can confirm whether the app uses GA4F or AdMob. The problem with this approach is that it does not capture any information about the class member that could be used to determine what conduct, if any, they were exposed to. For example, Mr. Hochman's methodology does not account for:

- app developers who use multiple SDKs;
- users who did not have any private information sent to Google even though they used analytics-enabled apps, within the meaning of Plaintiffs' claims, such that they did not suffer the alleged injury;

[275] Hochman Report, ¶ 344.
[276] Hochman Report, ¶ 345.
[277] Hochman Report, ¶ 349.

reliably shows account holders' (s)WAA status. However, as I explained above, his method of identifying sWAA-off data and associating that with specific users is unreliable.

237. Mr. Hochman has no factual basis for his opinion that Google can delete any products, services, or algorithms that it built with (s)WAA-off data. Setting aside his vague and problematic definition of sWAA-off data, and what would be encompassed in Google's "purge," his ideas on how Google can purge its systems of (s)WAA-off data are disconnected from the reality of how Google works and what users expect from these settings. Furthermore, Hochman recommends that Google purge all data without regard to the status of other settings and consents by both end users and Firebase customers, that may affect how this data can be used. His recommendation assumes things about Google's infrastructure that are beyond the scope of this case and what Mr. Hochman and I were asked to opine on.

238. Mr. Hochman is attempting to recreate how the (s)WAA controls function, not match their function to their disclosures. If Google were to accept Hochman's practices, it would no longer do the work Google says they do.

John Black
May 31, 2023